Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1 – 24. (Canceled)

25. (Currently amended) A method for detecting attacks on a data communications network, the method comprising:

assigning unassigned addresses to an intrusion detection sensor (IDS), such that any traffic directed at an unassigned address automatically arrives at the IDS;

using ~~an intrusion detection sensor~~ the IDS comprising intrusion detection code for:

monitoring data traffic on the network comprising a first group of addresses assigned to known users, and a second group of addresses that are not assigned to the known users;

identifying an address belonging to the second group of addresses;

spoofing a reply to a request associated with the identified address in order to detect data indicative of an attack;

listening for a response to the spoofing;

determining from the response that the request is suspicious;

generating an alert signal instructing a router to reroute the data traffic originating at the address assigned to the system transmitting the suspicious request to a disinfection address on the network; and

sending an alert message to the disinfection address, wherein said alert message comprises attack identity data; and

billing an entity for execution of at least one of the method steps, the charge being billed determined in dependence of one of: a size of the network, a number of the second group of the addresses monitored, a number of the first group of the addresses monitored, a volume of the data traffic inspected, a number of attacks identified, a number of the alert messages generated, a signature of the identified attack, a volume of rerouted data traffic, a degree of network security achieved, and a turnover of said entity.

26. (Previously presented) The method of claim 25 wherein the step of determining from the response comprises receiving no response within a specified time period.

27. (Previously presented) The method of claim 25 wherein the step of determining from the response comprises receiving the response within a specified time period and comparing said response to the attack identity data stored in memory, wherein the memory stores signatures identifying known attacks.

28. (Previously presented) The method of claim 25 wherein sending the alert message comprising the attack identity data comprises sending data indicative of signatures of identified known attacks.

29. (Previously presented) The method of claim 25 wherein the monitoring step comprises listening only for the data traffic directed to the second group of addresses.

30. (Currently amended) A method comprising steps of:

assigning unassigned addresses to an intrusion detection sensor (IDS), such that any traffic directed at an unassigned address automatically arrives at the IDS;

using a disinfection server for:

receiving an alert message sent from an intrusion detection sensor, said alert message comprising data indicative of signatures of identified known attacks for identifying a system originating data indicative of a network attack;

sending a warning message to an address assigned to the system, wherein said warning message comprises program code for eliminating the network attack when executed by the system originating the data indicative of the attack;

supporting an entity in handling of the detected attack by one of providing instructions for use of, assistance in executing, and execution of disinfection program code; and

providing a report to the entity containing information related to one of alert, disinfection, rerouting, logging, and discarding of data traffic in the context of the detected attack.